United Nations A/CN.9/965

General Assembly

Distr.: General
23 November 2018

Original: English

United Nations Commission on International Trade Law
Fifty-second session
Vienna, 8–26 July 2019

Report of Working Group IV (Electronic Commerce) on the work of its fifty-seventh session (Vienna, 19–23 November 2018)

I. Introduction

1. Background information on the work of the Working Group on legal issues related to identity management (IdM) systems and trust services may be found in working paper A/CN.9/WG.IV/WP.152, paragraphs 6–17. Following the Working Group's recommendation (A/CN.9/936, para. 95), the Commission requested the Working Group to conduct work on legal issues relating to IdM and trust services with a view to preparing a text aimed at facilitating cross-border recognition of IdM and trust services.[1] The Commission's request is framed in terms sufficiently broad to include aspects of the legal treatment of IdM and trust services additional to those already identified by the Working Group at its earlier sessions.

II. Organization of the session

2. The Working Group, composed of all States members of the Commission, held its fifty-seventh session in Vienna from 19 to 23 November 2018. The session was attended by representatives of the following States members of the Working Group: Armenia, Austria, Belarus, Brazil, Bulgaria, Burundi, Canada, China, Czechia, Ecuador, El Salvador, France, Germany, Greece, Hungary, Iran (Islamic Republic of), Italy, Japan, Kenya, Malaysia, Mexico, Pakistan, Poland, Republic of Korea, Russian Federation, Singapore, Spain, Switzerland, Thailand, Turkey, Uganda, United Kingdom of Great Britain and Northern Ireland, United States of America and Venezuela (Bolivarian Republic of).

3. The session was also attended by observers from the following States: Algeria, Belgium, Bolivia (Plurinational State of), Dominican Republic, Myanmar, Peru, Qatar, Sweden, Timor-Leste and Yemen.

4. The session was also attended by observers from the Holy See and the European Union.

[1] *Official Records of the General Assembly, Seventy-third Session, Supplement No. 17* (A/73/17), para. 159.

V.18-08227 (E) 041218 051218

Please recycle

5. The session was also attended by observers from the following international organizations:

(a) *United Nations system*: World Bank;

(b) *Intergovernmental organizations*: Commonwealth Secretariat, Gulf Cooperation Council, and Organisation internationale de la Francophonie;

(c) *International non-governmental organizations*: Alumni Association of the Willem C. Vis International Commercial Arbitration Moot (MAA), Association Droit & Méditerranée (Jurimed), Brazilian Chamber of Electronic Commerce (Camara-e.net), Centre for International Legal Education (University of Pittsburgh) (CILE), European Multi-channel and Online Trade Association (EMOTA), GSM Association (GSMA), Institute of Law and Technology (Masaryk University), International Federation of Freight Forwarders Associations (FIATA), International Trademark Association (INTA), International Union of Notaries (UINL), Jerusalem Arbitration Center (JAC) and Law Association for Asia and the Pacific (LAWASIA).

6. The Working Group elected the following officers:

Chairperson: Ms. Giusella Dolores FINOCCHIARO (Italy)

Rapporteur: Mr. Tomas KOZAREK (Czechia)

7. The Working Group had before it the following documents: (a) annotated provisional agenda (A/CN.9/WG.IV/WP.152); (b) notes by the Secretariat on legal issues related to IdM and trust services (A/CN.9/WG.IV/WP.153 and A/CN.9/WG.IV/WP.154); and (c) a proposal by Germany containing a draft instrument on cross-border legal recognition of IdM and trust services and a table with a road map for discussion of legal aspects of IdM and trust services (A/CN.9/WG.IV/WP.155 and Add.1).

8. The Working Group adopted the following agenda:

1. Opening of the session.
2. Election of officers.
3. Adoption of the agenda.
4. Legal issues related to identity management and trust services.
5. Technical assistance and coordination.
6. Other business.
7. Adoption of the report.

III. Deliberations and decisions

9. The Working Group continued consideration of legal issues related to IdM and trust services on the basis of the documents listed in paragraph 7 above. The deliberations and decisions of the Working Group on that topic are found in chapter IV of this report.

IV. Legal issues related to identity management and trust services

A. Scope of work

10. Acknowledging that the foundational identity of physical and legal persons was a matter for States to address, the Working Group confirmed that its work should focus on issues of transactional identity and, in that context, on issues of recognition rather than attribution of identity. At the same time, the Working Group recognized

that foundational identity issues might be relevant for its work since foundational identity might be required by law or used by contracting parties for establishing transactional identity.

11. The Working Group discussed whether its work should focus on facilitating reliable identification of both subjects and objects of transactions and confirmed that a clear distinction between the two concepts — subjects and objects — should be maintained. It was acknowledged that the identification of objects might be necessary to identify subjects of transactions, i.e. persons to whom rights, obligations and liabilities arising from transactions would be attributed. At the same time, it was said that an object did not have legal personality and could not bear liability.

12. Support was expressed for the view that issues of liability would be relevant to the work by the Working Group only to the extent that they touched upon liability arising from identification services. In particular, it was stressed that the discussion of liability of objects was outside the scope of work of the Working Group. At the same time, the view was expressed that the Working Group might touch upon responsibilities of object creators, such as the responsibility to properly identify the object at the time of its creation and to establish a clear link between the object and the person that would be liable for the object's actions, since those responsibilities could be relevant for the proper identification of persons.

13. With respect to paragraphs 5 and 6 of document A/CN.9/WG.IV/WP.153, a concern was expressed that they attempted to broaden the mandate of the Working Group's work on IdM. The view was expressed that the scope of the work by the Working Group on that topic should be narrowed down to issues on which the work could be accomplished within a reasonable period. The possibility of separating the topic into several sub-topics and delivering work products on those sub-topics at different points of time was not excluded.

14. Concern was expressed about the use of the term "trust services" in the working papers before the Working Group. The preference was expressed for the use of another term, such as "trusted services providers", which would better convey the intended meaning given that the word "trust" had a settled legal meaning in certain jurisdictions (see also para. 101 below).

15. Recalling the discussion at the previous sessions, the view was reiterated that the work by the Working Group on IdM should not try to establish functionally equivalent requirements for identification in the paper-based and in the electronic environments.

16. The view was expressed that the goal of the work should be to identify elements of IdM systems that facilitated the recognition of the outcome of identification across various IdM systems. It was explained that, without imposing any solution on contracting parties, the Working Group should therefore strive to provide a toolbox of options from which contracting parties might choose depending on their needs.

17. A question was asked about the reference to identification of traders operating in the informal sector contained in paragraph 11 of document A/CN.9/WG.IV/WP.153. It was indicated that the reference reflected a consideration expressed at the fifty-sixth session of the Working Group (see A/CN.9/936, para. 63) based on the concern that relying exclusively on public identity credentials might penalize those traders that faced significant challenges in obtaining formal recognition. It was added that economic and financial inclusion was one of the considerations being taken into account by UNCITRAL.

18. It was responded that that reference should not be seen as an endorsement of the informal sector and that it was preferable to encourage the transition of informal traders to the formal sector by considering entities with legal personality only. In that respect, it was recalled that providing the legal tools to facilitate the transition from the informal to the formal economy was the subject of the work by UNCITRAL Working Group I.

19. It was further noted that the object of the work of the Working Group was to facilitate reliable identification of entities regardless of whether they operated in the formal or informal sector. In that context, the point was made that various means of identification, which would not necessarily include public identity credentials, could be accepted by contracting parties depending on commercial risks at stake in a particular transaction.

B. Legal recognition requirements and mechanisms

20. A question was raised on whether legal recognition was needed to facilitate cross-border recognition of IdM systems at the global level or other type of recognition, such as technical recognition, would be sufficient. A question was also asked on the relationship between legal and factual recognition.

21. In response, it was noted that some level of trust was desirable before entering into commercial electronic transactions to better assess risks and reduce transaction costs. It was also noted that parties to a transaction seeking a higher level of legal certainty would pursue legal recognition of identification and that the overall goal of the Working Group was to increase trust in the use of digital identity. It was added that ex ante legal recognition would be one of the means to build trust.

22. It was indicated that the Working Group should focus on identifying the requirements of legal recognition and should not deal with technical aspects due to their constant evolution. It was further indicated that the work of the Working Group should neither introduce new obligations to identify nor affect existing ones (see also para. 110 below).

23. It was said that legal recognition of IdM systems may lower transaction costs given that the credentials issued under a system would be recognized without further assessment. It was also said that an efficient legal recognition mechanism should avoid the need for a double assessment, for instance in the originating and in the receiving jurisdictions.

24. It was indicated that the object of legal recognition was the preliminary question to address. It was explained that legal recognition could refer to recognition of IdM systems, of identity credentials or of the outcome of the identification process (see also A/CN.9/WG.IV/WP.153, paras. 57–58).

25. It was said that granting legal recognition to the outcome of the identification process could better address different approaches to identification, in particular in jurisdictions that did not make reference to the notion of level of assurance. It was added that legal recognition of outcomes was necessary to overcome reciprocity concerns that could arise with respect to legal recognition of IdM systems.

26. On the other hand, it was explained that recognition of IdM systems might facilitate recognition of credentials that, in turn, might facilitate recognition of the transaction where the credentials were used, i.e. the outcome of the identification process. Hence, it was indicated that the legal recognition of all those elements was complementary. It was added that recognition of credentials or of the outcome of the identification process should be possible where recognition of IdM systems was not.

27. It was added that public and private IdM systems were widely used and that a harmonized description of applicable levels of assurance, based on a set of rules and policies, was necessary to ensure the legal recognition of those IdM systems and increase the trust of business partners.

28. It was indicated that another preliminary question pertained to the effects of legal recognition. Reference was made to the options listed in paragraph 55 of document A/CN.9/WG.IV/WP.153. In response to a query, it was explained that the words "granting the same legal status as in the receiving jurisdiction, regardless of any foreign element" contained in that paragraph referred to granting legal

recognition without consideration of any foreign element involved (the "national treatment" principle).

29. A concern was raised that the reference to the notion of the originating jurisdiction contained in paragraph 55 of document A/CN.9/WG.IV/WP.153 could violate the principle of system neutrality in cross-border legal recognition of digital identity by implying the mandatory use of public IdM systems and credentials. In response, it was said that that notion referred to the law applicable to the IdM system used, which could also be multinational, regardless of its private or public nature.

30. It was said that granting national treatment was the preferable approach given that the presence of a foreign element should not per se be a reason to discriminate in international trade. It was added that another reason favouring such approach was that judges and other authorities could face difficulties in applying foreign laws and legal notions.

31. It was also said that, given the existence of national sets of requirements for IdM systems, the only feasible approach to legal recognition was the definition of its legal effects in a dedicated instrument.

32. Another view was that the effects of legal recognition would depend on the reliability of the IdM system used. In that line, it was explained that the use of an IdM system complying with a higher level of assurance could facilitate its cross-border legal recognition.

33. It was indicated that further clarification was needed on the legal effects of recognition. For example, it was suggested to clarify whether and under which conditions the statutory limitation of the liability of an identity services provider under a certain national law chosen by the parties to a commercial transaction could be upheld in another jurisdiction.

34. The question was raised on which entity should carry out any assessment necessary for legal recognition. It was stressed that most commercial transactions did not involve public authorities. In response, it was said that the assessment could be carried out by public entities, by accredited third parties, by dedicated organizations or by the parties to the commercial transaction.

35. It was further indicated that, while the assessment necessary for legal recognition could be carried out by private parties, the existence of an enabling legislative framework was necessary to provide legal recognition. It was added that, absent that legislative framework, parties' agreement on the law applicable to identification might not be upheld.

36. In response to a query, it was clarified that the draft provisions contained in the working papers before the Working Group had an illustrative nature at the early stage of the Working Group deliberations, without prejudice to their possible future detailed consideration.

37. It was explained that the decision to recognize IdM systems was based on trust, and that the essential elements needed to build such trust were the fundamental issue for discussion in the Working Group. It was further explained that trust could come from experience or as a result of the participation in an environment of trust. It was suggested that the use of an environment of trust could promote a higher level of legal certainty and that the Working Group should therefore work on creating such environment by defining its essential elements. It was stated that those essential elements were the minimum set of appropriate rules on how IdM systems should work, including on audit, insurance, certification, liability, and termination or other changes in levels of assurance, and mechanisms to ensure and verify that participants followed those rules. It was indicated that such environment of trust would allow business actors to rely upon and recognize the outcomes of IdM systems.

38. It was stressed that needs of developing countries should be duly taken into consideration in order to ensure the compatibility of any work product with all economic and legal systems and all levels of development. It was recalled that

one goal was to promote electronic commerce involving developing countries. It was indicated that the full implementation of the principle of technology neutrality was desirable to prevent the adoption of technical requirements that would be too costly or sophisticated for traders in developing countries.

39. A point was made that notification schemes were not alternative to levels of assurance. It was explained that the notification process involved the notification of IdM systems that conformed to pre-established standards as a step subsequent to the determination of a minimum set of rules and the assessment of IdM systems against those rules. A regional example combining notification schemes and levels of assurance was provided. It was explained that that example could be replicated for purely private sector purposes without the involvement of public authorities.

40. As regards specific legal recognition mechanisms, it was suggested that the Working Group should focus on the creation of a centralized minimal environment of trust, members of which would reach consensus on rules and policies that would underlie that environment. However, the view was also expressed that, although in theory desirable, it would be unrealistic to foresee the creation of a supranational body that would fulfil such functions.

41. Another view was that the Working Group should consider a legal recognition mechanism based on mapping and whitelisting of existing public and private accreditation schemes against parameters to be determined. It was explained that such parameters for privately run schemes might include, for example, the requirements for audit and insurance, and that the list of accredited schemes would not be exhaustive.

42. Views differed on whether the ex ante, the ex post or the mapping-based approach discussed in paragraphs 61 to 92 of document A/CN.9/WG.V/WP.153 should be taken. Positive and negative aspects of each approach were illustrated. It was considered important for the Working Group to identify those features of each approach acceptable to all States as well as problematic issues.

43. One view was that the mapping-based approach was preferable because of its flexibility in accommodating both ex ante and ex post legal recognition. Another view pointed at the advantages of ex post recognition given that legal operability would not be easy to achieve in jurisdictions lacking any IdM system. It was suggested that, due to cost-related and other considerations, business users in developing countries may favour legal recognition mechanisms that operated only in case of dispute, i.e. based on the ex post approach.

44. The prevailing view was that making the choice among those three approaches would be premature and undesirable: premature because of the insufficient experience with their use; and undesirable since all options should be retained to provide broader choice to business operators.

45. Moreover, making such choice was considered premature also because of the need to first identify obstacles to cross-border recognition of IdM systems. It was explained that, despite a widespread assumption that at a transactional level it would be beneficial and, in some cases, necessary for trading parties to have a higher level of trust in the identity of other parties, few cross-border recognition mechanisms of IdM systems existed. It was added that there could be different reasons for that situation, for example lack of information about the IdM system of the originating jurisdiction or because the results of the foreign assessment of the IdM system were not comparable or comprehensible. Identifying those reasons was considered essential to find appropriate legal solutions. In response, a question was raised whether obstacles indeed existed, or trading partners were comfortable with the status quo.

46. A point was also made that any solution should not be exclusive and that, while respecting legal requirements of any region or country, it should facilitate development and use of other options. It was noted that cost implications could determine which approach would prevail.

47. It was explained that those approaches were not mutually exclusive: for example, the mapping-based approach allowed both ex ante and ex post assessment of IdM systems against a predetermined set of rules. It was added that ex ante legal recognition was often used for the higher levels of assurance while ex post legal recognition was used for the lower levels. It was noted that legal presumptions and the burden of proof would vary with the level of assurance and would be known to the parties in advance to allow them to assess the consequences of relying on a particular approach.

48. Doubts were expressed that the mapping-based approach was a separate approach. Some delegations viewed the mapping as a step in an ex ante and ex post legal recognition. Other delegations considered the mapping-based approach a variation of an ex ante approach since it presupposed the existence of common rules agreed upon in advance by the participants in the mapping exercise and the involvement of a central public or private authority in the assessment.

49. Different views were expressed on the involvement of public authorities in a legal recognition mechanism. One view was that that involvement was desirable to support IdM systems offering a higher degree of trust. It was added that the involvement of public authorities could be useful to prevent the imposition of technical standards by larger market players on smaller ones. It was also indicated that the implementation of a cross-border recognition mechanism necessarily implied the involvement of public authorities due to its transnational nature.

50. Another view was that the involvement of public authorities in commercial transactions or the introduction of other forms of central control over those transactions should be limited. It was noted that significant cross-border electronic trade was already taking place without that involvement. It was suggested that further evidence based on experience should be made available to justify a bigger role of public authorities in cross-border recognition of IdM systems. The view was reiterated that the work on IdM should not proceed on the assumption that IdM systems and their legal recognition would necessarily or primarily be based on the involvement of public authorities, and that instead in the business-to-business context the focus should be on privately-run IdM systems and recognition.

51. Support was expressed for compiling more information on how different approaches worked in practice. In response, it was noted that UNCITRAL had prepared several successful texts in the area of electronic commerce based on limited business practice due to the novelty of the field. It was added that an UNCITRAL text on IdM systems and trust services could significantly contribute to modify the market structure and give new impulse to the use of those services.

52. In turn, it was observed that the experience in UNCITRAL demonstrated that an UNCITRAL instrument was particularly successful when it addressed a legal problem faced by the business community identified on the basis of empirical rather than theoretical knowledge. A suggestion was made to compile a list of actual problems that the UNCITRAL work on IdM would strive to address. The existence of divergent laws and approaches to IdM that raised the costs of doing business was considered one such problem that should be addressed through harmonization of laws, a task that fell under the mandate of UNCITRAL. Another problem cited was that in some cases a contracting party might be required to use a paper-based identification document for entering into an online commercial transaction. It was added that inadequate identification of the contracting party might create problems at the contract implementation stage. It was also noted that cross-border online identification posed challenges.

53. In response to a query, it was explained that the eIDAS Regulation had entered into force for the part relating to trust services in 2016 and for the part relating to IdM in September 2018. It was added that, while data was not available on its effects on the development of the IdM market given the limited time since entry into force, the effects on the development of the trust services market have already been significant.

54. In response to another query, it was explained that mapping exercises were difficult and time-consuming given also the challenges in comparing IdM systems developed on the basis of different sets of rules. It was added that the assessment of IdM systems was also costly and needed to be repeated regularly, typically on an annual basis. Another challenge, it was said, related to the frequent amendment of levels of assurance. It was further explained that the offer of private sector services for IdM systems assessment did not seem to point at a strong market demand for those services. Doubt was therefore expressed that the mapping-based approach would work at the global level. Another view was that mapping carried out by some States at the bilateral level, although time-consuming, was found very useful.

55. It was agreed that, while a decision on the most desirable mechanism for legal recognition was premature, the Working Group should continue its discussion on advantages and disadvantages of each model individually and in combination.

C. Levels of assurance

56. The Working Group discussed various aspects of the use of levels of assurance in IdM. It was explained that the level of assurance was an indicator of the level of confidence in the identification of an entity. It was added that reference to levels of assurance was critical to enable legal recognition mechanisms and that efforts should be made to harmonize the description of those levels. It was also explained that the number of levels of assurance to be made available corresponded to the number of legal effects sought, so that, for instance, if there were two legal effects associated with an IdM scheme (such as recognition or not), there would be two corresponding levels of assurance. It was also indicated that challenges related to the use of level of assurance included matching correctly those levels across borders as well as the need to frequently update them.

57. The view was expressed that a discussion on the definition of levels of assurance was premature and might involve technical issues. Broad support was expressed for the view that technical matters were outside the scope of the work of the Working Group. It was added that caution should be exercised as legal discussions could have significant implications on technological solutions. It was suggested that, if the progress of work so required, the assistance of relevant international organizations such as the International Telecommunications Union could be sought.

58. However, it was also said that the establishment of a legal recognition mechanism would require linking legal effects with properties, characteristics and attributes of the IdM system. It was added that that exercise should be outcome-based and not prescriptive and should aim at ensuring interoperability among levels of assurance.

59. It was suggested that a discussion of levels of assurance should clarify the legal consequences of the reference to those levels and that other consequences were irrelevant for the work of the Working Group. In that respect, it was indicated that the notion of levels of assurance had different legal consequences for IdM systems and for trust services. It was also indicated that different levels of assurance were associated with different legal effects, which satisfied different business needs.

60. The view was expressed that levels of assurance should be linked to discrete legal effects. However, the view was also expressed that it was not feasible to link levels of assurance with all possible legal effects. In response, it was indicated that it was possible and desirable to define a minimal set of legal effects associated with each level of assurance.

61. A question was asked on which legal effects were associated with the use of levels of assurance. Various examples were provided. It was indicated that the main legal effect was the association of a level of assurance with the reliability of the identification of a person or object (i.e. identification beyond reasonable doubt,

identification on a balance of probabilities, or failed identification), which was the core notion of the identification process.

D. Functional equivalence

62. Acknowledging that UNCITRAL made an important contribution to e-commerce development by formulating the principle of functional equivalence, the view was expressed that there could be a need for adjusting that principle to the IdM context. It was said that, while specific functions pursued by the notions of "writing", "original" and "handwritten signature" were easy to identify, it was difficult to point out the specific functions pursued by IdM. In that respect, it was noted that identification itself could be a function. The concern about attempts to establish functional equivalence between offline and online identification expressed earlier during the session (see para. 15 above) was reiterated.

63. It was suggested that provisions on IdM might need to refer to levels of assurance, degree of reliability or levels of equivalence and that provisions with different legal effects might therefore be needed for each level of assurance. It was pointed out that the "one size fits all" approach adopted in existing UNCITRAL provisions establishing functional equivalence might therefore not be appropriate in the IdM context.

64. Specific examples were provided illustrating the relationship between functional equivalence and the reference to levels of assurance in IdM. It was explained that different levels of assurance of identification might be required either by law or by contract also in the offline world. It was said that there was no consistent one-to-one match between each assurance level and offline identification.

65. The other view was that provisions on functional equivalence should not refer to levels of assurance since the latter raised technical aspects beyond the mandate of UNCITRAL, as was discussed during the session (see para. 57 above). The alternative view was that reference to levels of assurance was useful and the provisions should be redrafted to better convey that each level of assurance would produce different legal effects.

66. A question was put on whether the purpose of provisions on functional equivalence would be to establish equivalence in the legal status of online and offline IdM processes. It was pointed out that, in order to achieve that equivalence, a link with the offline IdM processes might need to be maintained in the provisions. Views differed on ways to establish that link.

67. The view was expressed that, unlike provisions on functional equivalence found in existing UNCITRAL texts that focused either on a thing (signature, writing or original) or on a state of affairs (possession), provisions on functional equivalence in the IdM context might need to focus on the IdM process. It was added that, while existing UNCITRAL provisions on functional equivalence aimed at confirming validity, in the IdM context there might be an interest to seek not only a binary answer to the question of legal recognition but also clarity on the legal effects of such recognition.

68. A question arose whether formulating specific functional equivalence provisions for each level of assurance would go beyond the functional equivalence principle by establishing rules on IdM. It was suggested that the draft provisions contained in paragraph 29 of document A/CN.9/WG.IV/WP.153 could have such effect.

69. Some support was expressed for the view that it was premature to discuss functional equivalence provisions until the scope of the work on IdM was clarified, in particular whether the work purported to achieve legal recognition of IdM processes or of the outcomes of those processes. It was noted that a functional equivalence provision would apply only if paper-based IdM was relevant. In addition, the suggestion was made to focus the discussion on an acceptable method of

identification instead of trying to elaborate narrow functional equivalence provisions to paper-based identification documents or processes. A point was also made that consideration of any drafting suggestions should be without prejudice to a decision by the Working Group on the form of a possible future text on IdM.

70. By way of preliminary remarks, it was noted that the opening wording in the draft provisions contained in paragraph 29 of document A/CN.9/WG.IV/WP.153 were misleading since, in the business-to-business context, law rarely required or permitted identification explicitly. It was explained that proper identification requirements in the business-to-business context might be implicit or simply dictated by business needs.

71. A suggestion was made to redraft the provisions as follows to reflect that different legal requirements and different levels of assurance might apply and that a decision was to be made on whether the scope of the work would encompass objects besides persons:

> "Where the law requires or permits the identification of [an entity] [person] [in a certain way], that requirement is met with respect to [electronic] [digital] identity management if a reliable method is used to [verify the [relevant] attributes of the [entity] [person] [at the same level or in the same way]]."

72. The need for defining certain terms used in the drafting suggestion, such as "a reliable method", was highlighted. It was also suggested that the provisions might need to be split into two, one containing the functional equivalence principle and the other dealing with reliability. Doubt was expressed that the provisions captured all elements of IdM. The need to capture all of those elements was stressed since deficiency in any link of the IdM chain might jeopardize the outcome.

73. It was suggested that the draft provisions contained in paragraph 29 of document A/CN.9/WG.IV/WP.153 could be redrafted as follows if they were to establish a functional equivalence to a physical identification document existing in the paper world (i.e., to a thing):

> "Where the law requires or permits the identification of a person with respect to a physical document, that requirement is met with respect to an electronic identification process if a reliable method is used to verify the relevant attributes of the person contained in that document."

74. It was indicated that IdM was a complex legal notion and that, if the provisions were to establish a functional equivalence to the IdM process, all composite elements thereof (e.g., identification and authentication) should be reflected. It was suggested that the draft provisions contained in paragraph 29 of document A/CN.9/WG.IV/WP.153 could as an example be redrafted as follows to include a reference to a "level of assurance" required under substantive law:

> "Where the law requires or permits the identification of a person on the balance of probabilities, that requirement is met with respect to an electronic identification process if a reliable method is used to verify the relevant attributes of the person to that same level."

75. Different views were expressed with respect to the drafting proposals contained in paragraphs 73 and 74 above, in particular: (a) whether specific reference to a physical or paper-based document was desirable. It was explained that in the physical world an authority in charge of identification of persons (e.g., a registry) would not necessarily produce physical identification documents but might itself be the authoritative source of identification information. It was also explained that the law might not stipulate whether paper-based or other identification means were to be used; and (b) that the notion of "balance of probabilities" was unknown and unclear. It was suggested that it might be replaced with reference to "the level of equivalence".

76. The proposal in paragraph 73 above was considered by some to be too narrow because it aimed only at establishing functional equivalence between paper-based

identification documents and electronic identification means. For those reasons, the proposal in paragraph 74 above was preferred by some.

77. In light of those comments, another drafting suggestion was made that purported to address concerns expressed on the draft provisions contained in paragraphs 73 and 74 above by merging and redrafting them:

> "Where the law or the parties require the identification of the entity or the person in accordance with a certain method, that requirement is met with respect to electronic identity management if a reliable method is used to verify the relevant attributes of the entity in accordance with the same level as assured by that method."

78. Another drafting proposal read as follows:

> "Where the parties wish or are required by law to perform the identification of a [person][subject], the application of an electronic identification procedure for this purpose has the equivalent legal effect as the application of non-electronic procedures recognized for this purpose, if the electronic identification procedure uses a reliable method to verify the attributes of the [person] [subject] relevant for this purpose."

79. Recalling that UNCITRAL texts already contained functional equivalence rules for certain trust services, namely for electronic signatures and for retention and archiving, the Working Group considered whether specific provisions should be prepared for each type of trust service, or, alternatively, a general rule on functional equivalence of IdM for all trust services could or should be drafted. The prevailing view was that specific functional equivalence provisions should be prepared for each trust service to accommodate their specific functions and that, in order to do so, a list of trust services should be compiled.

80. The value of digitalization of identities of legal persons for cross-border transactions was highlighted. It was stated that facilitating dematerialization of identification might be one of the goals of the work of the Working Group on IdM in addition to cross-border recognition of IdM systems. It was explained that in the former context, functional equivalence remained an important principle while levels of assurance or degrees of reliability were more relevant for recognition of IdM systems. A point was made that functional equivalence was an important concept also because it ensured no change in substantive law requirements.

81. After discussion, it was agreed to further consider whether degrees of identification or levels of assurance should be discussed in conjunction with functional equivalence provisions or provisions on a reliable method of identification. It was pointed out that provisions on functional equivalence, levels of assurance and mutual recognition formed the core of any future document. It was further stated that those provisions might need to be drafted taking into account various contexts, including the need for regulatory compliance, party autonomy, non-discrimination between online and offline means of identification and cross-border recognition of online identification.

82. Recognizing that the discussion of functional equivalence provisions on IdM could benefit from reference to cases where IdM was used, the Working Group heard examples when IdM was required in the business-to-business context, in particular for regulatory compliance (e.g. KYC), to establish the validity of a commercial document and to comply with contractual obligations. Concern was expressed that most examples provided did not refer to business-to-business transactions and that those that did refer to those transactions addressed issues of regulatory compliance or operation in highly-regulated sectors such as financial services. Doubts were in particular expressed that the KYC example was useful to IdM in the business-to-business context since KYC requirements, including identification of the customer, pursued specific goals related to the fight against terrorism financing, money-laundering and corruption.

83. A question was asked with respect to the entities relevant for the work of the Working Group (see A/CN.9/WG.IV/WP.153, para. 12). Support was expressed for the view that the work should focus on business-to-business relations and aim at facilitating trust in the identity of business partners. It was explained that transactions with public entities involved in trade (e.g. in the context of paperless trade facilitation) would also be relevant.

84. It was recalled that commercial transactions might fall under the scope of application of regulations containing an obligation to identify. In that respect, it was noted that regulatory requirements were likely to have an impact on the development of business practices. It was added that a future work product on IdM by the Working Group was unlikely to be significantly relevant in highly-regulated sectors.

85. It was recognized that IdM systems established in contexts other than business-to-business might be relevant to commercial partners and should therefore be taken into account in the work by the Working Group on IdM. It was reiterated that the primary focus of the Working Group should nevertheless be IdM in business-to-business transactions.

E. Consideration of a draft instrument and a road map contained in the proposal by Germany (A/CN.9/WG.IV/WP.155 and Add.1)

86. The Working Group heard an introduction of the proposal contained in documents A/CN.9/WG.IV/WP.155 and Add.1, which highlighted its main elements and the objectives pursued. Appreciation was expressed for the introduction and the comprehensive approach taken in the documents. The documents were found helpful for further discussion.

87. Clarifications were sought with respect to some provisions contained in the documents that did not appear applicable to business-to-business transactions, such as examples of primary identification in draft article 2 and reference to website authentication in draft article 19. A query was also raised whether business expressed any interest in establishing and supporting the functioning of the Coordinating Council referred to in draft article 5, the understanding being that such Coordinating Council might be established by non-State as well as State actors.

88. Concern was expressed with respect to draft provisions that deferred legislative functions to the Coordinating Council, including on matters raising public policy considerations. A view was expressed that States were often reluctant to delegate formulation of legal rules on such matters to a privately-run body. A query was also raised on whether the mechanism envisaged in document A/CN.9/WG.IV/WP.155 was to apply in the domestic or cross-border context or both.

89. In response, it was clarified that primary identification was typically used for establishing a legal entity and that website certificates were used in the business-to-business context, in particular in the subcontracting chain. As regards the Coordinating Council, it was clarified that such body could be publicly or privately run. An example of a body established in one jurisdiction with significant international outreach was provided. It was acknowledged that the involvement of States in the Council or in validating and enforcing its work would be essential. Ways to achieve that, it was noted, could be different, ranging from an international agreement to incorporating the code of conduct prepared by the Council in domestic legislation or providing incentives for its use.

F. Definitions

90. It was noted that the definition of "identity" contained in paragraph 17 of document A/CN.9/WG.IV/WP.153 might need to be amended in light of the earlier discussion of the Working Group on objects (see paras. 11–12 above). A question was raised whether that definition, unlike the definition of "identification", was necessary

or it should be deferred to national law. In response, it was stated that the definition of "identity" was useful as well.

91. With respect to the definition of "identity management" contained in paragraph 19 of the same document, concern was expressed that, as drafted, it might indicate that the cumulative reference to identification, authentication and authorization was necessary to define that concept whereas any of those listed elements would be sufficient. It was stated that the definition of "electronic identification" found in document A/CN.9/WG.IV/WP.144 was preferred.

92. A question was raised about the meaning of the word "environment" in the definition of "identity system" contained in paragraph 20 of document A/CN.9/WG.IV/WP.153. It was indicated that the definition of "electronic identification scheme" found in document A/CN.9/WG.IV/WP.144 was preferred.

93. With reference to the definition of "levels of assurance", it was suggested that the draft provisions in paragraphs 23 and 24 of document A/CN.9/WG.IV/WP.153 could be merged or a revised definition of that term could be built on paragraph 23. Another view was that there was no need for the definition of that term.

94. Views differed on whether work on legal recognition of IdM should refer to IdM processes, outcomes of those processes or both. The view was expressed that distinguishing between trust services and IdM would be necessary: in case of trust services, recognition would be sought for the outcomes while in the IdM context, recognition would be sought for processes. It was therefore suggested that at the initial stage work should focus on recognition of IdM processes and that it could be later decided to deal with recognition of individual IdM transactions. Some support was expressed for the view that work on recognition of IdM processes should proceed separately from work on recognition of outcomes of trust services.

95. The other view was that it would be inappropriate to separate the recognition of outcomes from the recognition of processes. It was recalled that IdM systems already existed but the absence of knowledge about the quality of the processes underlying them prevented the widespread recognition across borders of the outcomes of those systems.

96. Another view was that focus of work should only be on the recognition of outcomes of IdM processes. A further view was that, while focus of work should indeed be on establishing the equivalence of outcomes, the need for assurance of adequate processes should not be discarded.

97. Another view was that in practice it would be unrealistic to seek recognition of each outcome of IdM processes and trust services. It was therefore suggested that work should focus on the evidence-based recognition of processes (i.e., sets of rules), which might in turn lead to the automatic recognition of all outcomes of the recognized processes, thus dispensing with the need to seek recognition of each single outcome.

98. The prevailing view was that the Working Group should focus on recognition of processes and outcomes in the context of both IdM systems and trust services. It was considered essential to link that discussion with the discussion of approaches to legal recognition (see section B above).

99. Concern was expressed that definitions were being discussed by the Working Group before agreement had been reached on some essential substantive points. One view was that the definitions compiled in document A/CN.9/WG.IV/WP.150 were useful and sufficient at the current stage of deliberations. Another view was that definitions in documents A/CN.9/WG.IV/WP.144 and A/CN.9/WG.IV/WP.155 should be used instead of, or in combination with, the terms defined in documents A/CN.9/WG.IV/WP.150 and A/CN.9/WG.IV/WP.153.

100. The prevailing view was that the common understanding of essential terms for the work on IdM and trust services should be achieved at the earlier stage and a list of definitions would therefore be helpful. Accordingly, the Secretariat was requested

to include the definitions found in document A/CN.9/WG.IV/WP.144 in the list of essential definitions for future reference. It was also requested to cross-refer in that list to document A/CN.9/WG.IV/WP.150 and to the definitions in document A/CN.9/WG.IV/WP.155. It was further requested to clarify the origin of the definitions and the extent of their consideration by the Working Group. The understanding was that definitions so consolidated would be preliminary and would be amended as the work progressed. A view was expressed that the Working Group should decide soon on the form of a legal text to be prepared in order to facilitate progress of work, among others, on definitions and to avoid repetitive discussions.

G. Trust services

101. The view was reiterated that reference should be made to "trusted service" to avoid any ambiguity with respect to the well-settled legal notion of "trust" (see para. 14 above).

102. The view was expressed that little evidence existed on the need to create cross-border mechanisms for the recognition of trust services, which were usually subject to contractual agreements. It was indicated that the work of the Working Group should be limited accordingly.

103. The view was also expressed that the trust services market clearly pointed at the need to provide a higher level of legal certainty on the cross-border use of trust services. It was added that work in the field of trust services was therefore of great importance and should be conducted in parallel with the work on IdM.

104. It was suggested that an open-ended list of trust services should be compiled based on a common definition of "trust service". It was further suggested that the definition of "trust service" contained in document A/CN.9/WG.IV/WP.144 should be used as a working hypothesis for future deliberations.

105. It was indicated that the trust services listed in document A/CN.9/WG.IV/WP.154 on the basis of existing legislation were: electronic signatures; electronic seals; electronic timestamps; electronic registered delivery services; website authentication; and electronic archiving. It was suggested that electronic escrow services could be added to that list. The suggestion was also made to add blockchain services to that list. In response, it was indicated that blockchain was a technology and not a service.

106. It was explained that the notion of levels of assurance should not be used with respect to trust services, since electronic identification means offering a high level of assurance could be used for trust services with different levels of reliability.

H. Other general principles

107. The importance of the principle of non-discrimination against the use of electronic means was stressed. It was noted that the draft provisions contained in paragraph 26 of document A/CN.9/WG.IV/WP.153 posed challenges by referring to verification of identity with respect to both IdM and trust services. It was suggested that those provisions should be redrafted to avoid any confusion or that two different provisions, respectively for IdM and for trust services, should be drafted.

108. It was suggested that any reference to an element of the process in the draft provisions on non-discrimination should be replaced with references to the outcome of that process. In that respect, it was suggested that the provisions relating to IdM should refer to "results of the verification of identity" and that the provisions relating to trust services should refer to "results of the application of trust services".

109. With respect to the drafting suggestions on party autonomy and the accompanying commentary, the following changes were proposed: (a) to amend the draft provisions contained in paragraph 42 of document A/CN.9/WG.IV/WP.153 to

reflect discussions in the Working Group as regards the scope of work (persons or objects; see paras. 11–12 above); (b) to replace the words "person controlling" in paragraph 44 of that document with the words "person legally responsible" on the understanding that the controller might not be the person legally responsible for the object; and (c) to identify core rules that parties might not vary or derogate from in order to increase certainty and predictability of cross-border recognition of IdM and trust services.

110. With reference to a drafting suggestion on the principle of no new obligation to identify, a point was made that a close link existed between that provision and the principle of party autonomy. It was explained that the principle of no new obligation to identify was broader than the principle of party autonomy since it also conveyed that no amendments to substantive law were intended. At the same time, it was noted that new obligations to identify might arise because of the use of a particular trust service but, in any case, the use of that trust service should take place on a voluntary basis (see also para. 22 above).

111. The importance of the work on IdM and trust services for enabling the production of evidence across borders was highlighted. It was also stressed that contractual agreements were subject to mandatory law.

I. Certification of IdM and trust service providers

112. The view was expressed that in the business-to-business context, it would be appropriate to offer all certification options, which included: no certification; self-certification; certification by an independent third party; certification by an accredited independent third party; and certification by a State body. It was explained that business partners should be able to choose the option most appropriate for their needs, recognizing that each option would produce different legal effects. It was further explained that a possible architecture for such voluntary certification would not necessarily involve public entities but might rely on independent certification.

113. A question was raised on how the results of such third-party certification would be recognized across borders other than by enforcing a contractual clause. In response, the International Accreditation Forum was identified as an example of a body that facilitated recognition of certificates.

114. Concern was expressed that any solution presupposing a central certification, accreditation or oversight body might not be appropriate in situations where distributed ledger technology was involved in IdM and trust services because of challenges in identifying the body able to request the certification and the body to assess, among others. It was noted that the liability regime in those situations was also unclear.

115. A view was expressed that provisions on certification should not place an excessive burden on IdM service providers. In addition, it was stated that the State oversight over activities of private sector certifying bodies was essential to prevent risks to competition and abuse, in particular with respect to small market players. It was observed that accreditation of certifying bodies with State authorities aimed at ensuring independence, impartiality and fairness. In that respect, it was suggested that independent authorities might be in a better position to achieve those goals.

J. Liability

116. It was explained that the issue of liability could be dealt with in different manners depending on the scope of work. On the one hand, if the goal was to facilitate cross-border recognition of IdM and trust services, it would be necessary to determine the applicable law. On the other hand, if the goal was to provide guidance at the national level, for instance in the form of a model law, a discussion on liability allocation could be necessary, bearing in mind that the parties themselves could agree

on allocation of liability. In the latter case, it was added, a discussion of limitation of liability could also be necessary.

117. It was indicated that, as a general principle, service providers should be held liable for the services they provided. It was added that that general principle should apply to both IdM service providers and trust service providers. It was explained that higher quality services were provided at a higher cost, and that for that reason it could be possible to presume the intention or negligence of providers of those services in case of damage arising from the use of their services.

118. Recalling that the work of the Working Group focused on transactional identity, a question was raised with respect to possible liability of public entities. It was explained that public entities might be held liable as supervisory authorities and as service providers. It was added that the question of their liability might also arise when transactional identity credentials issued by private service providers relied on foundational identity credentials provided by public authorities.

K. Institutional cooperation mechanisms

119. The role of institutional cooperation mechanisms in achieving mutual legal recognition and interoperability of IdM systems and trust services was noted. It was also noted that there might be different forms of such mechanisms, which could be of a private or public nature. The view was expressed that in any scenario of such institutional cooperation, objective criteria and a mechanism for verification of compliance with those criteria would be necessary. It was added that any decision on institutional cooperation mechanisms should take into account the views of the private sector.

120. With respect to paragraph 39 of document A/CN.9/WG.IV/WP.154, the suggestion was made that reference to the common technical framework should be replaced with reference to interoperability not to jeopardize the principle of technology neutrality. The views were expressed that harmonization of legal rules and both contractual and legislative frameworks contributed to the establishment of the common legal framework.

L. Transparency

121. It was stated that transparency should be understood in terms of clarity and disclosure of terms and conditions of services, code of conduct by service providers (i.e., their operational policies) and assessment reports. It was explained that disclosure might be to subscribers, the general public or supervising authorities, as appropriate, subject to protection of any confidential information.

122. It was said that transparency of terms and conditions of services was important to allow subscribers to make an informed choice among competing market offers. It was added that it was also considered important for competitors, for example in evaluating their offers against those of other market players, and for other stakeholders, for instance to monitor competition in the market.

123. It was noted that another aspect of transparency pertained to notification of security breaches, which could impact not only systems but also transactions. It was explained that a proper security breach notification mechanism was considered important for improving performance and increasing the level of confidence.

124. It was noted that a number of regulations, including on data protection, would be applicable in the transparency context.

M. Data retention

125. The view was reiterated that privacy and data retention were important topics but that they fell outside the scope of the mandate received by the Working Group. It was indicated that the outcome of the work of the Working Group should not attempt to modify existing law in those or other fields.

126. The importance of electronic archiving services for business was noted. It was explained that electronic archiving pursued the specific function of providing legal certainty on the validity of archived electronic records in case of dispute and for other needs. It was suggested that the legal recognition mechanism for electronic archiving could be limited to ensuring compliance with the legal requirements of the jurisdiction where the archived records needed to be used.

N. Supervision of service providers

127. There was agreement that the discussion of supervision aspects should be held together with that of certification (see section I above). It was recognized that, while many aspects would be common for both certification and supervision, differences existed and should be reflected in terminology and provisions addressing those two subjects. One distinct feature of supervision was considered to be the need for taking corrective and enforcement actions in case of non-compliance with mandatory requirements.

128. The view was reiterated that the role of State supervising authorities as the only bodies that could ensure stability and proper supervision should not be underestimated. The difference between supervision and control, including self-control and control by other market players and subscribers of services, was highlighted. It was also noted that the role of State authorities was growing not only in supervision but also in development and deployment of IdM systems and in the provision of IdM and trust services, which would necessitate separating those functions of public authorities. It was considered premature to reach a conclusion on whether any particular model of supervision, public or private (contractual), would be necessary.

129. The difficulty of supervising distributed ledger technology was mentioned since, for instance, there could be no central provider to supervise. It was also noted that taking corrective and enforcement actions in those situations would be problematic, including by introducing changes in a public blockchain system through a "hard fork" or otherwise.

O. Decisions of the Working Group under agenda item 4

130. The view was expressed that future documents prepared by the Secretariat should contain additional draft provisions on core issues in order to further facilitate progress. It was added that those draft provisions should refer to the various possible options, rely on existing legislative texts and proposals submitted by States and International Organisations to the Working Group, and be prepared with the assistance of experts.

131. The view was also expressed that future documents should focus on identifying core questions useful to fully understand the scope of the project and provide analysis and research needed to make informed choices.

132. It was noted that the two suggested approaches were compatible and that both were useful. It was recalled that a firm timeline for submission of documents applied, which might not allow for carrying out broad intersessional expert consultations.

133. The Working Group asked the Secretariat to prepare documents for its fifty-eighth session on the basis of the existing ones, by drafting new provisions on

core issues as well as identifying and illustrating key questions for the Working Group and bearing in mind the applicable time frame.

V. Technical assistance and coordination

134. The Working Group heard an oral report by the Secretariat on technical assistance and cooperation activities undertaken since the oral report by the Secretariat at the previous session of the Working Group. Reference was made, in particular, to treaty actions with respect to the United Nations Convention on the Use of Electronic Communications in International Contracts (New York, 23 November 2005)[2] and activities of the Secretariat on the promotion of UNCITRAL electronic commerce texts, including in cooperation with other bodies, such as the United Nations Economic and Social Commission for Asia and the Pacific (UN/ESCAP) and the United Nations Conference on Trade and Development (UNCTAD). Reference was made to the work carried out by the Secretariat on illustrating the interaction between UNCITRAL texts, on the one hand, and relevant provisions of free trade agreements, on the other hand.

135. The Working Group was also informed about past and upcoming electronic commerce-related events organized or attended by the Secretariat in furtherance of the mandate received from the Commission to compile information on legal issues related to the digital economy.[3] An invitation was extended to States and other organizations to participate in or otherwise contribute to those activities.

136. Appreciation was expressed for the information provided and the activities undertaken by the Secretariat on technical assistance and cooperation in the area of electronic commerce law. It was noted that, besides preparation of legal texts, activities aimed at promoting broader adoption, understanding and use of those texts as well as coordination were essential to ensure the achievement of UNCITRAL's mandate.

---

[2] United Nations, *Treaty Series*, vol. 2898, No. 50525.

[3] *Official Records of the General Assembly, Seventy-third Session, Supplement No. 17* (A/73/17), para. 253(b).